

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

---

#### **REMARKS**

The Examiner is thanked for the thorough examination of the present application. While Applicants respectfully disagree with the rejection of the claims set forth in the final Office Action for the reasons discussed in the Amendment After Final filed July 16, 2004, to further prosecution independent Claims 11, 17, 25, and 30 have been amended to further define the subject matter thereof over the prior art. Support for the amendments may be found on pages 12 and 14 of the originally filed specification and in FIG. 4, for example. No new matter is being added.

In view of the amendments and the arguments presented in detail below, it is submitted that all of the claims are patentable.

#### **I. The Claimed Invention**

The present invention is directed to an electronic circuit for a cryptography coprocessor. As recited in amended independent Claim 17, for example, the electronic circuit includes a plurality of input/output registers having a scrambling register for receiving digital key data. More particularly, the digital key data includes an unencrypted digital key and a plurality of scrambling bits intermixed with the unencrypted digital key. The electronic circuit further includes an input register for receiving message data to be processed by the encryption or decryption operation, and a key register for receiving the digital key data for use in the

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

---

encryption or decryption operation. A multiplexer transfers data between the plurality of input/output registers and the input register and the key register. Additionally, a dedicated two-way link connects the multiplexer and the scrambling register for transferring the scrambling bits therebetween substantially simultaneously with the transfer of data between the battery of input/output registers and the multiplexer. Moreover, a processor is connected to the scrambling register, the input register, and the key register and performs the encryption or decryption operation on the message data in the input register based upon the digital key data and the scrambling bits. The electronic circuit further includes a controller for controlling the plurality of input/output registers, the multiplexer and the processor, and an output register to transmit the result of the encryption or decryption operation to the plurality of input/output registers through the multiplexer.

The intermixed scrambling bits advantageously secure the loading of the digital key into the input/output registers. Yet, by separately storing the scrambling bits in the scrambling register, the processor may readily determine the digital key from the contents of the key register and the scrambling register, as discussed on pages 12 and 13 of the originally filed specification, for example. Independent Claim 11 is directed to a related electronic circuit, and independent Claims 25 and 30 are directed to related methods. Similar to Claim 17, each of these claims recites that the scrambling bits are intermixed with the digital key, as well as using a dedicated two-way link for transferring the scrambling bits between the multiplexer and

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

---

scrambling register substantially simultaneously with the transfer of data between the battery of input/output registers and said multiplexer.

## **II. The Claims Are Patentable**

The Examiner rejected independent Claims 11, 17, 25, and 30 based upon the prior art illustrated in FIG. 3 of the application and U.S. Patent No. 6,144,744 to Smith, Sr. et al. (hereafter "Smith"). While the Examiner acknowledges that the prior art shown in FIG. 3 of the present application fails to teach or fairly suggest intermixing scrambling bits with a digital key, the Examiner contends that Smith provides this noted deficiency.

Smith discloses a method and apparatus for securely transferring objects (i.e., master keys) between different cryptographic processing modules. The master key transfer is accomplished using the Dieffie-Hellman key exchange protocol which allows a module to create a transport key for encrypting items to be transferred to a receiving module. Thus, the method of Smith allows the two modules to build a transport key to securely transfer a master key encrypted with the transport key.

The Examiner contended in the final Office Action that a BTK register 1614 discussed at col. 16, lines 13-36 of Smith is equivalent to the scrambling register, and that this BTK register receives digital key data comprising a digital key and scrambling bits intermixed therewith, as recited in the above-noted independent claims. As support for this contention, the Examiner

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

---

simply points to the above-noted text of Smith, which is reproduced below for convenience:

"FIG. 17 shows the general procedure 1700 for transferring a key part (such as MK1 or AMK1) from one crypto module 102 to another.

First, using the procedure to be described below, an authority establishes a basic transport key (BTK) as a shared secret between the source and target modules 102 (step 1702). At the end of this step, the transport key BTK is stored in the BTK register 1614 of each crypto module 102 involved in the transfer, but is not itself accessible to the authority 104.

The authority 104 then extracts the key part from the appropriate master key register of the source module 102, using the Extract and Encrypt Master Key (XEM) command 116 described below (step 1704). Referring also to FIG. 18, this command 116 encrypts the key part in question ("source key") under the transport key BTK in register 1614 and places the result in EBX register 1616, where it is freely available to the requesting authority 104; a hash pattern of the extracted key is also placed in BXHP register 1618.

Thereafter, the authority loads the key part that it has obtained in encrypted form into the appropriate master key register of the target module 102, using the Load Key Part (LKP) command 116 described below (step 1706). Referring also to FIG. 19, this command 116 decrypts the key part under the transport key BTK in the register 1614 of the target module 102 and places the result in the appropriate master key register of that module." Smith, col. 16, lines 10-35.

Thus, the basic transport key stored in the BTK

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

---

register 1614 is merely a secret key which is used to encrypt part of a master key. Nowhere does Smith teach or fairly suggest that the BTK register 1614 is an input/output scrambling register which separately stores scrambling bits apart from a digital key with which the scrambling bits are previously intermixed. Indeed, the above-quoted text of Smith indicates that the BTK register 1614 only stores the basic transport key, and nothing else. While Smith teaches performing encryption using the basic transport key, and also generating key hashes, nowhere does it teach or fairly suggest intermixing scrambling bits with a digital key to create digital key data, and then separately storing the scrambling bits in an input/output scrambling register for later use by a processing module to determine the digital key.

In addition to the foregoing differences, the above-noted independent claims have also been amended to recite using a dedicated two-way link for transferring the scrambling bits between the multiplexer and scrambling register substantially simultaneously with the transfer of data between the battery of input/output registers and said multiplexer. This feature is not taught or fairly suggested by any of the prior art of record. Accordingly, taken as a whole, the prior art of record fails to teach or fairly suggest all of the recitations of the above-noted independent claims.

Accordingly, it is submitted that independent Claims 11, 17, 25, and 30 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art

In re Patent Application of  
**LIARDET ET AL.**  
Serial No. 09/506,158  
Filed: **FEBRUARY 17, 2000**

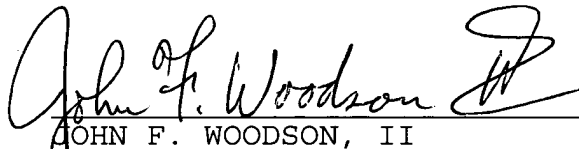
---

and require no further discussion herein.

**CONCLUSIONS**

In view of the foregoing, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



JOHN F. WOODSON, II  
Reg. No. 45,236  
Allen, Dyer, Doppelt, Milbrath  
& Gilchrist, P.A.  
255 S. Orange Avenue, Suite 1401  
Post Office Box 3791  
Orlando, Florida 32802  
Telephone: 407/841-2330  
Fax: 407/841-2343  
Attorney for Applicants